(3) 24

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2002-169912

(43)Date of publication of application : 14.06.2002

---

(51)Int.Cl. G06F 17/60
G09C 1/00
H04L 9/32
H04N 7/16
H04N 7/173

---

(21)Application number : 2000-365576 (71)Applicant : HITACHI LTD

(22)Date of filing : 30.11.2000 (72)Inventor : MARUYAMA JUNICHI
KANEHIRA AKIRA
TSUNEHIRO TAKASHI
TSUNODA MOTOYASU
IGUCHI SHINYA
MIZUSHIMA EIGA

---

(54) CRYPTOGRAM DECODER, FEE CHARGING APPARATUS AND CONTENTS DELIVERY SYSTEM

(57)Abstract:
PROBLEM TO BE SOLVED: To charge on an as-used basis for the use of contents while protecting the copyrights for onerous contents in a contents delivery system.
SOLUTION: In the contents delivery system, a contents delivery server 120 deliver contents while encrypting them, a contents reproducing apparatus 110 uses a

charging apparatus 130 to decode the encrypted contents. The fee charging apparatus 130 has a counter of numerical value of values to restrict the use of the decoding process and when the counter performs the decoding process, the counter is increased or decreased on the as-used basis for the use according to attributes of the contents. A user can add the numerical value of values to the fee charging apparatus 130 by paying the consideration.

CLAIMS

[Claim(s)]

[Claim 1]A code decoding device which has a means to perform code decoding processing which decrypts and outputs inputted coding information, comprising:
A memory measure which stores control information which controls execution of said code decoding processing, and is tolerant to unlawful access.
A means to update control information stored in said memory measure according to an attribute provided in quantity of information and this information which were processed by said code decoding processing.
A means to restrict when a permission is granted based on said control information, and to permit execution of said code decoding processing.

[Claim 2]An authentication means which attests a communications partner which inputs and outputs information in the code decoding device according to claim 1, respectively, A code decoding device having further an encryption communication means which restricts when each communications partner is attested by said authentication means as a suitable communications partner, performs an input and an output of information, enciphers these input and output, respectively and is performed further when communicating with said communications partner.

[Claim 3]Input which should perform said code decoding processing in the code

decoding device according to claim 1 or 2 is information divided into two or more information components, A code decoding device characterized by updating said control information based on attribution information of the information component when it has attribution information for each [which was divided] this information component of every and said code decoding processing is performed to an information component.

[Claim 4]A code decoding device, wherein said control information contains an index showing a remuneration of information which performed said code decoding processing in a code decoding device of any one statement of three from claim 1.

[Claim 5]A charging device charged at a holder of this information according to a remuneration of acquired information, comprising:

A means to perform code decoding processing which decrypts and outputs enciphered input.

A memory measure which stores a value value showing value for payment of a remuneration of information to acquire.

A means to decrease a value equivalent to a remuneration of acquired information from a value value stored in said memory measure according to quantity of information and the attribute of this information which carried out decoding processing and were acquired by said code decoding processing.

A means to restrict when said value value is beyond a predetermined value, and to permit execution of said code decoding processing.

[Claim 6]A means by which it has the following and said contents playback device transmits a Request to Send of contents directed by user to said contents distribution server, A means to publish contents playback device keys, and a means to acquire contents data enciphered by said contents playback device keys outputted from said charging device, Decrypt contents data enciphered by said contents playback device keys using said contents playback device keys, have a means to acquire contents of a plaintext, and said charging device, A means to publish a charging device key, and a means to acquire double enciphered content outputted from said contents distribution server, A means to acquire contents data which decrypted this double enciphered content using a charging device key, and was enciphered by said contents playback device keys, A contents distribution system provided with a means to send contents data enciphered by said contents playback device keys to said contents playback device.

A contents distribution server for distributing arbitrary contents, being a contents distribution system charged to acquisition of these contents, and accumulating and distributing contents.

A contents playback device for acquiring and outputting said contents.

A means by which it has a charging device for charging when acquiring said contents,

and said contents distribution server receives a contents Request to Send transmitted from said contents playback device.
A means to acquire contents playback device keys which said contents playback device publishes, A means to encipher contents which enciphered a means to acquire a charging device key which said charging device publishes, and contents demanded by said contents Request to Send by said contents playback device keys, and were this enciphered further with said charging device key, and to output as double enciphered content.

[Claim 7]The contents distribution system comprising according to claim 6:
Said contents distribution server has a means to distribute at least one or more contents simultaneously in parallel to at least one or more contents playback devices, and said contents playback device, A means to acquire at least one or more contents from at least one or more contents distribution servers simultaneously in parallel.
A means to reproduce at least one or more contents simultaneously in parallel.
A means which can perform said acquisition means and a reproduction means simultaneously in parallel.

[Claim 8]In the contents distribution system according to claim 6 or 7, said charging device, A memory measure which stores a value value showing value for payment of a remuneration of information to decrypt, A means to decrease a value which is equivalent to a remuneration of acquired information from a value value stored in said memory measure according to quantity of information and the attribute of this information which carried out decoding processing and were acquired, A contents distribution system having further a means to restrict when said value value is beyond a predetermined value, and to permit execution of said code decoding processing.
[Claim 9]Contents distributed in the contents distribution system according to claim 7 or 8 are the information divided into two or more information components, Have attribution information for each [which was divided] this information component of every, and said charging device, A contents distribution system decreasing a value which is equivalent to a remuneration of acquired information from a value value stored in said memory measure according to the amount of information of an information component and the attribute of this information component which carried out decoding processing and were acquired when decoding processing is performed to an information component.
[Claim 10]A contents distribution system having further a means to which a value value stored in a memory measure of said charging device is made to increase from claim 7 in a contents distribution system of any one statement of nine.
[Claim 11]In a contents distribution system of any one statement of ten, from claim 7, said contents distribution server, A contents distribution system having a means to

acquire position information on said contents playback device, and distributing contents according to a position of said contents playback device when distributing contents.

[Claim 12]Contents which said contents distribution server distributes in a contents distribution system of any one statement of 11 from claim 7, A contents distribution system characterized by making a value value within said memory measure increase when said charging device carries out decoding processing of the contents to which this value value is made to increase including a thing to which said value value is made to increase.

[Claim 13]In a contents distribution system of any one statement of 12 from claim 7, Have a coordinator who distributes contents to which contents which decrease said value, and said value value are made to increase, and said coordinator, Have said contents distribution server and supply of said contents is received from a contents holder, Execute distribution of contents, and collection of a price by proxy, and a fee is received from a contents holder to the remuneration, A contents distribution system receiving supply of advertising content from an advertising client, executing distribution of advertising content by proxy, and receiving an advertising rate from an advertising client to the remuneration.

[Claim 14]A contents distribution server characterized by comprising the following for accumulating and distributing contents, A contents distribution method in a contents distribution system provided with a contents playback device for acquiring and outputting said contents, and a charging device for charging when acquiring said contents.

A step which acquires contents enciphered from said contents distribution server, decrypts this enciphered contents with said charging device, and acquires contents of a plaintext.

A step which updates a value value which expresses value for payment of a remuneration currently held in said charging device when decryption is performed with said charging device.

DETAILED DESCRIPTION

[Detailed Description of the Invention]

[0001]

[Field of the Invention]This invention the contents data of an audio, video, or a text stored in the server, It is related with the contents distribution system using the charging device which enables fee collection to the copyright protection and onerous contents of contents especially, and said charging device about the art suitably

distributed to the contents playback device which a user possesses.

[0002]

[Description of the Prior Art]In recent years, the trial which is going to distribute the contents data of an audio, video, etc. via networks, such as the Internet, is made. This prepares the contents distribution server which accumulated contents, and a user accesses a contents distribution server via a network from the terminal of PC etc., The contents made into the purpose are acquired out of the contents accumulated in the contents distribution server, it is a system which pays a remuneration by payment systems, such as a credit card, for example, a system like a statement is proposed by JP,11-96237,A. In this system, the technique of having a database of the content acquisition history for every user, and a contents distribution server managing the fee collection produced with distribution of contents data, dividing and bundling up by a month unit etc., and performing the settlement of accounts by a credit card is taken. In this system, the so-called contents distribution of streaming form was also supported, contents data was divided into the small unit, the distributing server managed distribution of data in detail for every small unit, and charging has realized meter-rate system fee collection.

[0003]

[Problem(s) to be Solved by the Invention]Since the contents data treated with the above contents distribution systems is digitized and the duplicate is easy, It is important for providing the function prevent from using except the device which has a just right, or establishing the device which prevents the 3rd person's tapping also in the transmission and reception of data performed via a network etc. to protect the copyright of contents.

[0004]In the system which distributes onerous contents data, the collection means of the price for contents poses a problem. For example, when a means to check that contents acquisition has been completed certainly is needed and acquisition of contents is interrupted for the system which pays a fee collectively for a certain reason after acquiring contents, procedures, such as re connection, will be needed and processing will become complicated. Although there is also a charging method in the form of how much per acquisition of one contents stream about the so-called contents of streaming form, even if it ends viewing and listening on the way in this case, there is a problem that all fee collection will be performed.

[0005]Although there is a meter-rate system charging system charged according to the quantity which uses contents which are proposed in JP,11-96237,A mentioned above, for example by one of the methods for solving these problems, In the payment system which manages a fee collection situation like this system by the hysteresis information which a contents distribution server possesses, and performs accounting using a credit card. Time difference arises between that a user needs to register with a server beforehand to system use and the exchange of contents, and settlement of

accounts, and inconvenience, like the amount of money by which the user was charged cannot be known in real time arises.

[0006]this invention is made in view of said situation, and comes out. The purpose is to provide the contents distribution system which has a function which protects the copyright of **, and an accounting function of the contents by the meter-rate system.

[0007]

[Means for Solving the Problem]In order to attain the above-mentioned purpose, this invention is characterized by that a code decoding device which has a means to perform code decoding processing which decrypts and outputs inputted coding information comprises:

A memory measure which stores control information which controls execution of said code decoding processing, and is tolerant to unlawful access.

A means to update control information stored in said memory measure according to an attribute provided in quantity of information and this information which were processed by said code decoding processing.

A means to restrict when a permission is granted based on said control information, and to permit execution of said code decoding processing.

[0008]An authentication means for which this invention attests a communications partner which inputs and outputs information in the above-mentioned code decoding device, respectively, When communicating with said communications partner, it had further an encryption communication means which restricts when each communications partner is attested by said authentication means as a suitable communications partner, performs an input and an output of information, enciphers these input and output, respectively and is performed further. It prevents using contents unjustly except a device which has a just right by this.

[0009]This invention is the information divided into an information component of plurality [input / which should perform said code decoding processing] in the above-mentioned code decoding device, When it has attribution information for each [which was divided] this information component of every and said code decoding processing is performed to an information component, said control information is updated based on attribution information of the information component.

[0010]This invention is characterized by that a charging device charged at a holder of this information according to a remuneration of acquired information comprises:

A means to perform code decoding processing which decrypts and outputs enciphered input.

A memory measure which stores a value value showing value for payment of a remuneration of information to acquire.

A means to decrease a value equivalent to a remuneration of acquired information

from a value value stored in said memory measure according to quantity of information and the attribute of this information which carried out decoding processing and were acquired by said code decoding processing.
A means to restrict when said value value is beyond a predetermined value, and to permit execution of said code decoding processing.

[0011]A contents distribution server for this invention distributing arbitrary contents, and being a contents distribution system charged to acquisition of these contents, and accumulating and distributing contents, Have a contents playback device for acquiring and outputting said contents, and a charging device for charging when acquiring said contents, and said contents distribution server, A means to receive a contents Request to Send transmitted from said contents playback device, A means to acquire contents playback device keys which said contents playback device publishes, A means to acquire a charging device key which said charging device publishes, and contents demanded by said contents Request to Send are enciphered by said contents playback device keys, Furthermore, encipher enciphered this contents with said charging device key, have a means to output as double enciphered content, and said contents playback device, A means to transmit a Request to Send of contents directed by user to said contents distribution server, a means to publish contents playback device keys, and a means to acquire contents data enciphered by said contents playback device keys outputted from said charging device, Decrypt contents data enciphered by said contents playback device keys using said contents playback device keys, have a means to acquire contents of a plaintext, and said charging device, A means to publish a charging device key, and a means to acquire double enciphered content outputted from said contents distribution server, This double enciphered content was decrypted using a charging device key, and it has a means to acquire contents data enciphered by said contents playback device keys, and a means to send contents data enciphered by said contents playback device keys to said contents playback device.
[0012]This invention is characterized by that the above-mentioned contents distribution system comprises:
Said contents distribution server has a means to distribute at least one or more contents simultaneously in parallel to at least one or more contents playback devices, and said contents playback device, A means to acquire at least one or more contents from at least one or more contents distribution servers simultaneously in parallel.
A means to reproduce at least one or more contents simultaneously in parallel.
A means which can perform said acquisition means and a reproduction means simultaneously in parallel.

[0013]In the above-mentioned contents distribution system, this invention said

charging device, A memory measure which stores a value value showing value for payment of a remuneration of information to decrypt, A means to decrease a value which is equivalent to a remuneration of acquired information from a value value stored in said memory measure according to quantity of information and the attribute of this information which carried out decoding processing and were acquired, It restricted, when said value value was beyond a predetermined value, and it had further a means to permit execution of said code decoding processing.

[0014]This invention is the information for which contents distributed were divided into two or more information components in the above-mentioned contents distribution system, Have attribution information for each [which was divided] this information component of every, and said charging device, When decoding processing is performed to an information component, according to the amount of information of an information component and the attribute of this information component which carried out decoding processing and were acquired, a value which is equivalent to a remuneration of acquired information from a value value stored in said memory measure is decreased.

[0015]This invention was further provided with a means to which a value value stored in a memory measure of said charging device is made to increase in the above-mentioned contents distribution system.

[0016]In the above-mentioned contents distribution system, said contents distribution server is provided with a means to acquire position information on said contents playback device, and this invention distributes contents according to a position of said contents playback device when distributing contents.

[0017]Contents to which said contents distribution server distributes this invention in the above-mentioned contents distribution system, When said charging device carries out decoding processing of the contents to which this value value is made to increase including a thing to which said value value is made to increase, a value value within said memory measure is made to increase.

[0018]This invention has a coordinator who distributes contents to which contents which decrease said value, and said value value are made to increase in the above-mentioned contents distribution system, Said coordinator has said contents distribution server, and receives supply of said contents from a contents holder, Distribution of contents and collection of a price are executed by proxy, a fee is received from a contents holder to the remuneration, supply of advertising content is received from an advertising client, distribution of advertising content is executed by proxy, and an advertising rate is received from an advertising client to the remuneration.

[0019]A contents distribution server for this invention to accumulate and distribute contents furthermore, It is a contents distribution method in a contents distribution system provided with a contents playback device for acquiring and outputting said

contents, and a charging device for charging when acquiring said contents, A step which acquires contents enciphered from said contents distribution server, decrypts this enciphered contents with said charging device, and acquires contents of a plaintext, and when decryption is performed with said charging device, While having a step which updates a value value showing value for payment of a remuneration currently held in said charging device, said contents, When decrypted with contents which decrease said value value when decrypted with said charging device, and said charging device, contents to which said value value is made to increase with a plaintext are included.

[0020]

[Embodiment of the Invention]Hereafter, an embodiment of the invention is described using a drawing.

[0021]Drawing 1 is a figure showing the outline composition of the contents distribution system with which one embodiment of this invention was applied.

[0022]In drawing 1, the contents playback device 110, The function which plays contents, such as an audio, video, and a text, It is the device provided with the function which accesses the contents distribution server 120 and acquires contents, and has the charging device connecting means 111, the contents distribution server connecting means 112, the encryption communication means 113, the input means 114, and the contents playback means 115. The contents playback device 110 can take the gestalt of a portable viewer, a set top box, or PC, for example.

[0023]The contents distribution server 120 is a device which performs accumulation and distribution of contents, and has the contents playback device connecting means 121, the encryption communication means 122, the contents storage means 123, the contents encryption means 124, and the enciphered content distribution means 125. The contents distribution server 120 distributes contents suitably in response to the contents acquisition request from the contents playback device 110.

[0024]When the contents playback device 110 processes acquisition or reproduction of onerous contents, etc., the charging device 130 is a device to charge and has the contents playback device connecting means 131, the encryption communication means 132, the enciphered content decoding means 133, and the charging means 134. The charging device 130 may be made to build in the contents playback device 110, and is very good in the gestalt which can be freely detached and attached to the contents playback device 110. The charging device 130 may be made to add to recorders, such as an IC card and memory card, etc., or to add to magnetic recording media, such as a hard disk, as a gestalt like a semiconductor chip, and to provide this accounting function. It is good also as a gestalt which gives a wireless communication function like bluetooth and provides the contents playback device 110 with the above-mentioned function by non-contact communication.

[0025]The network 140 is a communication path of the contents playback device 110

and the contents distribution server 120, for example, is the Internet, an on-line system, or a wireless communication network. It is good as for what is different in the information transmission paths from the contents distribution server 120 to the contents playback device 110, and the information transmission paths from the contents playback device 110 to the contents distribution server 120. For example, satellite broadcasting, a cable TV network, etc. can be used for the former, and a telephone line, radio, etc. can also be used for the latter.

[0026]The outline of the process flow of the contents distribution system provided with the copyright protection function and meter-rate system accounting function which are realized by the aforementioned equipment configuration is as follows, for example.

[0027]The contents playback device 110 and the charging device 130 are connected using the charging device connecting means 111 and the contents playback device connecting means 131. Then, the contents distribution server 120 and the contents playback device 110 are connected using the contents playback device connecting means 121 and the contents distribution server connecting means 112.

[0028]After communication between devices is secured by the aforementioned means, as for the contents playback device 110 which received acquisition directions of the contents from a user by the input means 114, the distribution request of contents is first sent to the contents distribution server 120. The contents distribution server 120 which received it enciphers using the contents encryption means 124, and then transmits the applicable contents in the contents group accumulated in the contents storage means 123 to the contents playback device 110 using the enciphered content distribution means 125. Since it is unreproducible if the contents data enciphered here remains as it is, The contents playback device 110 decodes this enciphered content data using the enciphered content decoding means 133 of the charging device 130, and the charging device 130 performs fee collection to contents use by the charging means 134 simultaneously. Finally the contents playback device 110 reproduces the decrypted contents data using the contents playback means 115.

[0029]In order to secure the safety of communication between the devices performed in process of said processing, the encryption communication means 113, 122, and 132 are used. It is realizable by means to attest a communications partner with the encryption communication means said here, for example, means to publish the key for enciphering information to a communications partner, the means for decrypting the information which the communications partner enciphered using this key, and the group of **.

[0030]Next, the contents playback device 110 and the charging device 130 are explained still in detail among each device which constitutes this contents distribution system.

[0031]The contents playback device 110 is explained first.

[0032]Drawing 2 is a figure showing an example of the outline composition of the contents playback device 110. CPU201 controls each part of the contents playback device 110 in generalization. The memory 202 comprises a ROM and RAM. The program for CPU201 to control each part of this contents playback device 110 in generalization is stored in ROM. RAM functions as a work area of CPU201.

[0033]The communication apparatus 204 is used for accessing the contents distribution server 120. It may be a wireless communication means and may be a wire communication means. It may have two or more those means of communication. It may have a means to communicate with various devices, such as other contents playback devices 110 and PC, in addition to contents distribution server 120.

[0034]The input device 203 comprises various buttons and a touch panel, for example, and receives the reproduction instruction from a user, acquisition directions of contents data, etc. The display 208 comprises a liquid crystal panel, for example, displays the list of contents or displays the video content played with the video recovery device 207. The audio playback unit 206 decodes the enciphered contents, and obtains an audio signal. And an audio signal is outputted to a speaker (un-illustrating), external headphone, etc. in which it was contained by this contents playback device 110. The video recovery device 207 decodes the enciphered contents, and acquires a video signal. And a video signal is outputted to the display 208 in which it was contained by this contents playback device 110, an external monitor, etc.

[0035]The charging device contact 205 connects the charging device 130, data comes to hand from the charging device 130, or data is sent to the charging device 130. The interface 209 constitutes CPU201, the memory 202, and this contents playback device 110, and also manages the data transmission and reception between devices.

[0036]Next, the audio playback unit 206 is explained.

[0037]Drawing 3 is a figure showing the outline composition of the audio playback unit 206. The audio playback unit 206 has the dark decoding circuit 302, the decoder circuit 303, and the I/O circuit 301 for performing data transmission and reception with each part of this contents playback device 110 via the interface 209 so that it may illustrate.

[0038]The dark decoding circuit 302 has a mutual recognition function with an external device, and is provided with the function which enciphers, sends and receives data between said devices. The dark decoding circuit 302 has a means to publish an audio playback unit key, for example, considers the contents enciphered with this audio playback unit key as an input, decodes them with this audio playback unit key, and is outputted to the decoder circuit 303. The decoder circuit 303 accepts necessity, elongates and reproduces the audio information outputted from the dark decoding circuit 302, and obtains an audio signal. And an audio signal is outputted to a speaker etc. Each part which constitutes the audio playback unit 206 shown in a figure here is built and crowded, for example on 1 chip.

[0039]Next, the video recovery device 207 is explained.

[0040]Drawing 4 is a figure showing the outline composition of the video recovery device 207. The video recovery device 207 has the dark decoding circuit 402, the decoder circuit 403, and the I/O circuit 401 for performing data transmission and reception with each part of this contents playback device 110 via the interface 209 so that it may illustrate.

[0041]The dark decoding circuit 402 has a mutual recognition function with an external device, and is provided with the function which enciphers, sends and receives data between said devices. The dark decoding circuit 402 has a means to publish video recovery device keys, for example, considers the contents enciphered by these video recovery device keys as an input, decodes them with this audio playback unit key, and is outputted to the decoder circuit 403. The decoder circuit 403 accepts necessity, elongates and reproduces the video data outputted from the dark decoding circuit 402, and acquires a video signal. And a video signal is outputted to a display, a monitor, etc. Each part which constitutes the video recovery device 207 shown in a figure here is built and crowded, for example on 1 chip. The video recovery device 207 may be made to build in a video display device, and you may also be built and crowded on 1 chip in accordance with the audio playback unit 206 and the video recovery device 207. These playback equipment may be realized by software.

[0042]By subsequent explanation, an audio playback unit key and video recovery device keys are doubled, and it describes as contents playback device keys.

[0043]Drawing 5 is a figure showing the outline composition of the charging device 130. The charging device 130 has the dark decoding circuit 501, the fee collection circuit 502, the store circuit 505, and the I/O circuit 504 that is interfaces with the charging device contact 205.

[0044]The dark decoding circuit 501 has an authentication function and a dark decoding function. The value value counter 503 which restricts operation of the dark decoding circuit 501 is formed in the store circuit 505. The value value counter 503 has a means for memorizing the quantity of the value which the charging device 130 is accumulating. Value is a concept showing worth of contents, for example, it substitutes for money. The memory measure of the quantity of value may be made to decide for a counter to increase and for counters to decrease in number on the contrary, for example, if value increases. It can restrict, when the value of this value value counter 503 is in the predetermined range, and the dark decoding circuit 501 can perform said code decoding processing. That is, since a remuneration is paid with this value value when a user acquires charged contents, when there is no value value of beyond a predetermined value, as decoding processing cannot be performed, it has restricted so that acquisition of contents cannot be performed.

[0045]The fee collection circuit 502 has the function to change the value value counter 503 with the quantity and the attribute of the information processed by the

dark decoding circuit 501. The dark decoding circuit 501, the fee collection circuit 502, and the store circuit 505 are good here to store in what is called the Tampa resistant field (TRM: Tamper Resistant Module) 506 in order to strengthen security.

[0046]The dark decoding circuit 501, the fee collection circuit 502, etc. may be made the composition realized by the memory for, for example, storing the program which has said function, and said program, and CPU for executing said program.

[0047]It may be made for each part which constitutes said charging device 130 to be built and crowded, for example on 1 chip, or it may be made to comprise two or more chips. When it constitutes more than one from a chip, it is desirable to give a device which is not read in the exterior of the charging device 130 in the signal during a chip.

[0048]Next, an example of the procedure of the communication performed between each device in this contents distribution system is explained.

[0049]Drawing 6 is an example of 1 composition of the system charged at the time of reproduction of contents. Here, the contents playback device 110 and the charging device 130 have a means to publish the key for enciphering data, respectively, and a means for decrypting the data enciphered with this key. Each device may have a unique key beforehand for every device, and this key may create it with a random number etc. here each time. However, this key is made not to be known in addition to the just device to which possession was permitted by attestation.

[0050]The contents playback device 110 transmits the distribution request and the contents playback device keys Kp of contents to the contents distribution server 120 (601). Next, the charging device 130 transmits the charging device key Kc to the contents distribution server 120 (602). In response to it, the contents distribution server 120 enciphers the demanded contents D by the contents playback device keys Kp, and enciphers this enciphered content E (Kp, D) with the charging device key Kc further. Next, the contents distribution server 120 transmits this double enciphered content E (Kc, E (Kp, D)) to the charging device 130 (603). here, double enciphered content E (Kc, E (Kp, D)) remains as it is -- since it is unreproducible with the contents playback device 110 then, in order to reproduce contents, the charging device 130 is needed.

[0051]The charging device 130 decodes double enciphered content E (Kc, E (Kp, D)) which received with the charging device key Kc which self holds, and changes the counter V of a value value according to the throughput in that case (604). Then, the decrypted contents E (Kp, D) are transmitted to the contents playback device 110 (605). When the value value V which this charging device 130 holds takes the value of the predetermined range, the charging device 130 is prevented from decoding double enciphered content. Therefore, acquisition of a certain amount of [a user] value value for contents playback is needed.

[0052]The contents playback device 110 which received this enciphered content decodes this enciphered content E (Kp, D) by the contents playback device keys Kp

which self holds, and reproduces the contents D of the decrypted plaintext. Here, except contents playback device 110 with these contents playback device keys Kp, since enciphered content E (Kp, D) which the contents playback device 110 received cannot be decrypted, it can prevent an illegal copy.

[0053]In the above processing, the contents playback device keys Kp and the charging device key Kc are safely sent and received using the authentication function and encryption communication function which each device has.

[0054]The exchange shown above is expressed to drawing 7 in a flow chart. First, the contents playback device 110 requires own attestation of the both sides of the contents distribution server 120 and the charging device 130 (Steps 701-704). When attestation is performed normally, the contents playback device 110 transmits the contents playback device keys Kp to the contents distribution server 120 with the Request to Send of contents (Step 705). Attestation is continuously performed mutually between the contents distribution server 120 and the charging device 130 (Steps 705-709). When the contents distribution server 120 requires attestation of the charging device 130 and attestation is performed normally, the charging device 130 transmits an authentication demand and the charging device key Kc to the contents distribution server 120 (Step 708). In response to it, the demanded contents D are first enciphered by the contents playback device keys Kp, it enciphers with the charging device key Kc further, and the contents distribution server 120 transmits to the charging device 130 (Step 710). In response to it, the charging device 130 decrypts double enciphered content E (Kc, E (Kp, D)) once with the charging device key Kc, and transmits these contents E (Kp, D) to the contents playback device 110 (Step 711). Finally, the contents playback device 110 decrypts enciphered content E (Kp, D) which received by the contents playback device keys Kp, and reproduces the contents D (Step 712).

[0055]In said each procedure, when processing of attestation etc. is not performed normally, error handling (Step 713) is carried out and it ends.

[0056]Drawing 8 is a sequence diagram in the contents distribution system explained using drawing 6 and drawing 7 showing an example of the data transmission-and-reception procedure between devices.

[0057]In order that the contents playback device 110 may receive attestation from the contents distribution server 120, the authentication demand containing the certificate C of the public key KPp and public key of the contents playback device 110 (KPp) is transmitted to the contents distribution server 120 (801).

[0058]In response, the contents distribution server 120 verifies attestation of the contents playback device 110, and the justification of the public key KPp (802). Next, session key Ks1 is generated (803), this is enciphered by KPp, and it transmits to the contents playback device 110 (804).

[0059]The contents playback device 110 which received this decrypts Ks1 enciphered

with the secret key Kp, and obtains session key Ks1. After checking session key Ks1 (805), in order that the contents playback device 110 may receive attestation from the charging device 130 continuously, the authentication demand containing the certificate C of the public key KPd and public key of the contents playback device 110 (KPd) is transmitted to the charging device 130 (806).

[0060]In response, the charging device 130 verifies attestation of the contents playback device 110, and the justification of the public key KPd (807). Next, session key Ks2 is generated (808), this is enciphered by KPd, and it transmits to the contents playback device 110 (809).

[0061]The contents playback device 110 which received this decrypts Ks2 enciphered with the secret key Kp, and obtains session key Ks2. After checking session key Ks2 (810), the contents playback device 110, Then, session key Ks3 is generated (811) and a contents Request to Send including the information which enciphered the session keys Ks2 and Ks3 by session key Ks1 is transmitted to the contents distribution server 120 (812).

[0062]The contents distribution server 120 which received this is decrypted using session key Ks1, and obtains Ks2 and Ks3. After checking the session keys Ks2 and Ks3 (813), session key Ks4 is generated (814), and the contents distribution server 120 transmits own authentication data C (Server) to the charging device 130 in order to receive attestation in the charging device 130 continuously (815). Authentication data C (Server) is enciphered here using session key Ks2 with session key Ks4.

[0063]In response, the charging device 130 decodes authentication data C (Server) and session key Ks4 using session key Ks2, and performs attestation of the contents distribution server 120, and the check of session key Ks4 (816, 817). When attestation and a check are performed normally, own authentication data C (Charge) and the charging device key Kc are enciphered by session key Ks4, and it transmits to the contents distribution server 120 (818).

[0064]In response, the contents distribution server 120 decodes authentication data C (Charge) and the charging device key Kc using session key Ks4, and performs attestation of the charging device 130, and the check of the charging device key Kc (819, 820). When attestation and a check are performed normally, the double enciphered content data which enciphered the contents data D by session key Ks3, and was further enciphered with the charging device key Kc is transmitted to the charging device 130 (821).

[0065]In response, the charging device 130 decrypts double enciphered content data using the charging device key Kc, and obtains the contents data D enciphered by session key Ks3. And after changing the value value V based on the attribution information of this contents data (822), enciphered content data is transmitted to the contents playback device 110 (823).

[0066]In response, the contents playback device 110 decrypts enciphered content

data using session key Ks3, acquires the contents data D, and reproduces this contents data (824).

[0067]Next, an example of the contents distribution system with which this embodiment was applied to drawing 9 is shown. The charging device 130 has the function to charge by the meter-rate system, when it has an enciphered content decoding means and a charging means and decoding processing of enciphered content is performed as mentioned above. This charging means has the value value counter 503, and restricts said decoding processing with the value of the counter. For example, it restricts, when taking the value of the range with a counter, and said decoding processing is carried out as [be / available]. Or it may be made to change the function of the memory storage 906 with the value of a counter. For example, when a counter value is beyond constant value, it can make it possible to use a supplementary service in addition to the function of the charging device 130. The function to save the hysteresis information of contents acquisition, etc. in the store circuit 505 of the charging device 130 can also be provided. It can also process that it will be made to give a discount if the using frequency which is made not to charge is piled up when using again the contents for which this hysteresis information was used for example, which were charged once etc.

[0068]In this contents distribution system, a value value is an index showing worth of contents, it is set up and published by the contents holder 902, the coordinator 901, etc. so that worth of contents may be balanced, and it is added to contents as attribution information of contents. Transfer of the price between the contents holder 902 and user accompanying distribution of contents is performed via value. A user pays a remuneration and receives issue of value. The user can also purchase the charging device 130 beforehand supplemented with the value value, and can also fill up only a value value afterwards.

[0069]As shown in drawing 10, the variation of value value counter V can not only be collectively set up to the whole contents D, but it can set it to every [of contents] component (D1-D8). The small part of the contents divided, for example by unit time can be allotted to the component of the contents said here, and the variation alpha (Dx) of a value value will be set to it in this case according to the contents for every time of contents. The number of bits, the number of scenes, etc. of data can divide contents, and it can also be considered that each divided small part is the component Dx. By this, when it provides a user with the contents of an image, for example, fee collection can be set up selectively, and about an important scene or a popular scene, flexible meter-rate based fee collection, such as changing charge amount selectively, can be performed.

[0070]The limiting method of the code decoding processing according to value value counter V for example, If code decoding processing is performed, a value value will decrease, and when a counter is beyond constant value, it restricts, When it sets up

perform code decoding processing, the contents which added the attribute which makes a value value as shown in D1, D2, D3, D4, and D7 subtract are treated as onerous contents, The contents which added the attribute to which a value value as shown in D6 and D8 is made to increase can be treated as increase contents in value which give a privilege to the user who viewed and listened. By this, if onerous contents are seen, a value value will decrease, but service that a value value will increase if contents, such as an advertisement, are seen can also be provided.

[0071]A user may decide to be able to receive various services other than contents distribution by paying the value value of a charging device to a remuneration. For example, other articles may be acquirable to the remuneration of the payment of a value value.

[0072]The contents playback device 110 is a device provided with the function which plays contents, such as an audio, video, or a text, and the function which accesses the contents distribution server 120 and acquires contents as mentioned above. Radio, a cable, or its both may be sufficient as this means of communication. The contents playback device 110 contains the contact of the charging device 130, it is connecting here the charging device 130 which has a means relaying the communication performed between the contents distribution servers 120, and the acquisition and reproduction of onerous contents of it are attained. When reproducing gratis contents, it can also decide not to need connection of the charging device 130. The contents playback device 110 may be provided with the function which displays the counter of the value value in the charging device 130.

[0073]Although the example which accesses the one contents distribution server 120 explained in the example mentioned above, this contents playback device 110 and the charging device 130 access two or more contents distribution servers 120, and are good also as it being possible to acquire two or more contents simultaneously in parallel. It may have a means to reproduce two or more contents simultaneously in parallel. For example, divide the viewing area of a display, and another contents are reproduced on each divided screen, or separate audio contents and video content are reproduced simultaneously. It may have a means to perform said acquisition means and a reproduction means simultaneously in parallel. Change of the value value counter in the charging device 130 will also be performed simultaneously in parallel to the case where the aforementioned parallel processing is performed, for every contents.

[0074]The coordinator 901 has the contents distribution server 120 for distributing contents, It is a contractor who executes distribution of contents by proxy instead of the contents holder 902, and supply of contents is received and accumulated from the contents holder 902, and contents are suitably distributed according to the demand from the playback equipment 110 which a user owns. The coordinator 901 collects the remuneration of contents acquisition and use of distribution service from a user, and

pays the contents holder 902. In that case, the fee which executes distribution and price collection by proxy is received from the contents holder 902. The coordinator 901 receives the commission from the advertising client 903, and receives the remuneration (remuneration as an advertising agency) according to the quantity of the advertising content which distributed and distributed advertising content to the user. It is good to determine the advertising content which doubles, uses and distributes the distribution region information set as each advertising content, and the position information of the user of a distribution object when distributing advertising content. In this way, advertising effectiveness can be heightened by distributing the advertising content close to the area. Although the coordinator 901 distributes contents according to the demand from a user, he distributes simultaneously the advertising content selected on that occasion as mentioned above. The target contents themselves may be changed according to a user's position information.

[0075]The contents holder 902 is a contractor who acquires or manufactures contents, such as an audio, video, or a text, The value of contents is set up, the coordinator 901 is provided with this setup information with contents, and the remuneration is received according to the distributed amount of contents.

[0076]It is an advertisement provider who requests distribution of advertising content from the coordinator 901, and the advertising client 903 sets up the value of advertising content, it provides the coordinator 901 with this setup information with advertising content, and pays the remuneration according to the distributed amount of advertising content.

[0077]If the attribute of the increase in value is added to advertising content and advertising content is reproduced, privileges, like a coupon is saved can also be given.

[0078]The access point 904 has a connect function to the network 907, and a communication function with the contents playback device 110, When the direct access of the contents playback device 110 cannot be carried out to the network 907, it becomes repeating installation for the contents playback device 110 to access the network 907. A means to memorize the position information on the area in which the access point 904 was installed, When it has a means to transmit this position information to the contents distribution server 120 and communication between the contents playback device 110 and the contents distribution server 120 is performed, this position information is transmitted to the contents distribution server 120. The access point 904 and the contents distribution server 120 can also be used as the separate device whose number it can also equip and is one as shown in drawing 9. Wireless communication means, such as bluetooth and a cellular phone, may be sufficient as the means of communication of the access point 904 and the contents playback device 110, for example, and wire communication means, such as a telephone line, may be sufficient as it. For the signal transduction from the contents distribution server 120 to the contents playback device 110, terrestrial broadcasting,

The gestalt of using broadcast means, such as satellite broadcasting and cable TV, and using an access point for the signal transduction from the contents playback device 110 to the contents distribution server 120 may be sufficient.

[0079]KIOSK terminal 905 has the function to receive a remuneration and to supplement the charging device 130 with a value value, for example, is installed in a station, a convenience store, a record shop, etc. KIOSK terminal 905 has a function linked to the network 907, and the coordinator 901 can do an exchange of the charging device 130 and data via KIOSK terminal 905. It is a gestalt of a user removing the charging device 130 of a gestalt like an IC card from the contents playback device 110, inserting the charging device 130 in KIOSK terminal 905, doing predetermined operation, and connecting with the coordinator's 901 server. For example, the hysteresis information of contents acquisition is recorded on the charging device 130, and the coordinator 901 can also provide the function to guess the trend of a commercial scene, by totaling this hysteresis information via KIOSK terminal 905.

[0080]The memory storage 906 is memory storage which has a function linked to the network 907, is provided with the function to provide the storage area assigned for every user, and can use it as an external storage of the contents playback device 110. The memory storage 906 may be provided with the encryption communication apparatus for exchanging information with the contents distribution server 120, and the contents playback device 110 and the charging device 130 safely.

[0081]Next, the procedure which distributes advertising content using the access point indicated to drawing 9 is explained using drawing 11.

[0082]First, the contents playback device 110 connects with the contents distribution server 120 by access point 904 course (Step 1101-1102). The coordinator 901 specifies from which access point 904 the contents playback device 110 has accessed, and acquires the position information on this access point 904 here (Step 1103). Next, although the advertising content which transmits to the contents playback device 110 is determined using this position information, based on the distribution region information provided in each advertising content, contents suitable for the current position of the contents playback device 110 are chosen in this case (Step 1104). The advertising content finally determined by said means is enciphered in the procedure shown in drawing 6, and it transmits to the contents playback device 110 (Steps 1105-1107).

[0083]Drawing 12 is an example of 1 composition of the system charged at the time of acquisition of contents. Here, the memory storage 1200 and the charging device 130 have a means to publish the key for enciphering data, respectively, and a means for decrypting the data enciphered with this key. Each device may have a unique key beforehand for every device, and this key may create it with a random number etc. here each time. However, this key is made not to be known in addition to the just device to which possession was permitted by attestation. The memory storage 1200 is

the memory storage built in or connected to the contents playback device 110, for example.

[0084]The memory storage 1200 transmits the distribution request and the memory storage key Ks of contents to the contents distribution server 120 (1201). Next, the charging device 130 transmits the charging device key Kc to the contents distribution server 120 (1202). In response to it, the contents distribution server 120 enciphers the demanded contents D with the memory storage key Ks, and enciphers this enciphered content E (Ks, D) with the charging device key Kc further. Next, the contents distribution server 120 transmits this double enciphered content E (Kc, E (Ks, D)) to the charging device 130 (1203). here, double enciphered content E (Kc, E (Ks, D)) remains as it is -- since it is unreproducible with the contents playback device 110 then, in order to reproduce contents, the charging device 130 is needed.

[0085]The charging device 130 decodes double enciphered content E (Kc, E (Ks, D)) which received with the charging device key Kc which self holds, and changes the counter V of a value value according to the throughput in that case (1204). Then, the decrypted contents E (Ks, D) are transmitted to the memory storage 1200 (1205). When the value value V which this charging device 130 holds takes the value of the predetermined range, the charging device 130 is prevented from decoding double enciphered content.

[0086]The memory storage 1200 which received this enciphered content decodes this enciphered content E (Ks, D) with the memory storage key Ks which self holds, and acquires the contents D of the decrypted plaintext (1206). Here, except memory storage 1200 with this memory storage key Ks, since enciphered content E (Ks, D) which the memory storage 1200 received cannot be decrypted, it can prevent an illegal copy.

[0087]In the above processing, the memory storage key Ks and the charging device key Kc are safely sent and received using the authentication function and encryption communication function which each device has.

[0088]When moving contents to the contents playback device 110 from the memory storage 1200, the contents playback device 110 transmits contents playback device keys to memory storage, and using this key, the memory storage 1200 enciphers contents and transmits to the contents playback device 110.

[0089]Drawing 13 is a figure showing the example of 1 composition of the system charged at the time of reproduction of contents. Here, the contents playback device 110 and the charging device 130 have a means to publish the key for enciphering data, respectively, and a means for decrypting the data enciphered with this key. Each device may have a unique key beforehand for every device, and this key may create it with a random number etc. here each time. However, this key is made not to be known in addition to the just device to which possession was permitted by attestation.

[0090]The contents playback device 110 requires distribution of contents of the

contents distribution server 120 (1301), and requires transmission of the charging device key Kc of the charging device 130. In response to it, the charging device 130 transmits the charging device key Kc to the contents distribution server 120 (1302). In response to it, the contents distribution server 120 enciphers using the charging device key Kc, and transmits the demanded contents D to the memory storage 1300 (1303), and the memory storage 1300 stores enciphered content E (Kc, D) which received (1304).

[0091]Next, the contents playback device 110 transmits the contents playback device keys Kp to the charging device 130 (1305). Continuing, the memory storage 1300 transmits this enciphered content E (Kc, D) to the charging device 130 (1306). The charging device 130 decodes enciphered content E (Kc, D) which received with the charging device key Kc, and changes value value counter V according to the attribute of the contents D (1307). Next, the decrypted contents D are shortly enciphered by the contents playback device keys Kp, and it transmits to the contents playback device 110 (1308). The contents playback device 110 decrypts this enciphered content E (Kp, D) using the contents playback device keys Kp, and reproduces the contents D (1309).

[0092]Here, since enciphered content E (Kc, D) cannot be decrypted unless it uses the charging device key Kc, it can be safely kept on the memory storage 1300. A copy is also free. For this reason, the session (1301-1304) which transmits enciphered content E (Kc, D) to the memory storage 1300 from the contents distribution server 120, With the session (1305-1309) which transmits these contents E (Kc, D) to the contents playback device 110, it is separable.

[0093]The memory storage which may be built in the contents playback device 110 or the charging device 130, and is connected on the network may be sufficient as this memory storage 1300. In that case, the contents playback device 110 or the charging device 130 shall have the function to memorize a network address etc., for example, and shall have an accessing means to this memory storage 1300. The contents playback device 110 can share contents data between carrying out like this easily, also when it becomes unnecessary to build in mass memory storage and has two or more contents playback devices 110.

[0094]In the above processing, contents playback device keys and a charging device key are safely sent and received using the authentication function and encryption communication function which each device has.

[0095]In the above, one embodiment of this invention was described. This invention is not limited to the aforementioned embodiment and many modification is possible for it within the limits of the gist.

[0096]

[Effect of the Invention]As explained above, according to this invention, it becomes possible to perform contents distribution provided with the function which protects

contents copyright, and the function to charge suitably by the meter-rate system to use of contents according to the amount used. The contents from which a user can acquire a privilege if it views and listens to contents, and the suitable contents according to the user's position information can be distributed.

DESCRIPTION OF DRAWINGS

[Brief Description of the Drawings]

[Drawing 1]The figure showing the concept of this invention.

[Drawing 2]The figure showing the outline composition of a charging device.

[Drawing 3]The figure showing the outline composition of a contents playback device.

[Drawing 4]The figure showing the outline composition of an audio playback unit.

[Drawing 5]The figure showing the outline composition of a video recovery device.

[Drawing 6]The figure showing the contents distribution procedure of a contents distribution system.

[Drawing 7]The flow chart showing a contents distribution procedure.

[Drawing 8]The sequence diagram for explaining an example of an exchange of the data between a contents distribution server, a contents playback device, and a charging device.

[Drawing 9]The figure showing a general view of a contents distribution system.

[Drawing 10]The figure showing the concept of the attribution information of contents.

[Drawing 11]The flow chart showing the distribution procedure of the advertising content in a contents distribution system.

[Drawing 12]The figure showing the contents distribution procedure of a contents distribution system.

[Drawing 13]The figure showing the contents distribution procedure of a contents distribution system.

[Description of Notations]

110 -- Contents playback device

111 -- Charging device connecting means

112 -- Contents distribution server connecting means

113, 122, 132 -- Encryption communication means

114 -- Input means

115 -- Contents playback means

120 -- Contents distribution server

121 -- Contents playback device connecting means

123 -- Contents storage means

124 -- Contents encryption means

125 -- Enciphered content distribution means
130 -- Charging device
131 -- Contents playback device connecting means
133 -- Enciphered content decoding means
134 -- Charging means
201 -- CPU
202 -- Memory
203 -- Input device
204 -- Communication apparatus
205 -- Charging device contact
206 -- Audio playback unit
207 -- Video recovery device
208 -- Display
301, 401, 504 -- I/O circuit
302, 402, 501 -- Dark decoding circuit
303, 403 -- Decoder circuit
502 -- Fee collection circuit
503 -- Value value counter
505 -- Store circuit
506 -- Tampa resistant field
901 -- Coordinator
902 -- Contents holder
903 -- Advertising content
904 -- Access point
905 -- KIOSK terminal
906, 1200, 1300 -- Memory storage
907 -- Network
908 -- Means of communication